Kathleen Sullivan (SBN 242261)
kathleensullivan@quinnemanuel.com
QUINN EMANUEL URQUHART & SULLIVAN LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Sean S. Pak (SBN 219032)
seanpak@quinnemanuel.com
John M. Neukom (SBN 275887)
johnneukom@quinnemanuel.com.
QUINN EMANUEL URQUHART & SULLIVAN LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Steven Cherny *(admitted pro hac vice)*
steven.cherny@kirkland.com
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

[Additional counsel listed on signature page]

Attorneys for Plaintiff Cisco Systems, Inc.

KEKER & VAN NEST LLP
ROBERT A. VAN NEST - # 84065
rvannest@kvn.com
BRIAN L. FERRALL - # 160847
bferrall@kvn.com
DAVID J. SILBERT - # 173128
dsilbert@kvn.com
MICHAEL S. KWUN - # 198945
mkwun@kvn.com
633 Battery Street
San Francisco, CA 94111-1809
Telephone:415 391 5400
Facsimile: 415 397 7188
Attorneys for Defendant Arista Networks, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

CISCO SYSTEMS, INC.,

Plaintiff,

vs.

ARISTA NETWORKS, INC.,

Defendant.

CASE NO. 5:14-cv-5344-BLF

STIPULATION REGARDING ELECTRONIC DISCOVERY AND DOCUMENT PRODUCTION FORMAT

Unless otherwise agreed in a writing signed by the parties' counsel of record in this action, this Stipulation Regarding Electronic Discovery and Document Production Format ("Stipulation") shall govern the parties' discovery related to electronically stored information ("ESI")—as that term is used in Rule 34(a) of the Federal Rules of Civil Procedure—as well as the form of production of hard copy and source code documents. The discovery activities covered by this Stipulation are to be conducted as follows:

I. GENERAL PROVISIONS

1. This Stipulation supplements all other discovery rules and orders. It streamlines ESI production to promote a "just, speedy, and inexpensive determination" of this action, as required by Rule 1 of the Federal Rules of Civil Procedure.
2. This Stipulation may be modified for good cause. The parties may agree to modifications, and if so agreed to, shall jointly submit any modifications to the Court. If the parties cannot reach an agreement regarding proposed modifications, the parties shall submit their competing proposals and a summary of their dispute to the Court.
3. The parties have agreed that all electronic materials produced in this action will be exchanged electronically via secure FTP or on CD, DVD, flash drive or hard drive. To the extent the documents are ordinarily maintained by the producing party in a form that is electronically searchable, they must be produced in a form that is electronically searchable.

II. PRODUCTION OF HARD COPY DOCUMENTS

1. **PRODUCTION FORMAT.** The format of productions of hard copy documents shall comply with the following requirements:
    a. **IMAGE FORMAT.** Documents that exist in hard copy format only shall be scanned and produced as single page black and white Group IV TIFFs, created with a resolution of at least 300 dots per inch (dpi). Color documents may be produced in .JPG format in lieu of TIFF images; where

so produced, color JPG files should also be provided with a resolution of at least 300 dpi. Each TIFF or JPG image shall be branded with sequential production numbers and appropriate confidentiality designations. Each TIFF or JPG image filename shall correspond to the Bates number associated with that page. TIFF or JPG files shall show all text and images that would be visible to a user of the hard copy documents.

b. **DATABASE LOAD FILES/CROSS-REFERENCE FILES**. A production shall be provided with (a) an ASCII delimited data file (.dat) using Concordance default delimiters, and (b) an Opticon (Concordance Image) image load file (.opt) that can be loaded into Concordance version 8 or above. In addition:

   i. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the Image Load file(s) in the production.

   ii. The Opticon file should provide the beginning and ending Bates number of each document and the number of pages it comprises. Each TIFF or JPG in a production must be referenced in the corresponding image load file.

   iii. In addition to the metadata fields identified for production in II(1)(d) below, each .dat file shall include links to multi-page (document level) text files ("Text Path").

c. **OCR TEXT FILES.** A commercially acceptable technology for optical character recognition ("OCR") shall be used for all scanned, hard copy documents. The filename for the multi-page text file described above in II(1)(b)(iii) shall correspond to the beginning production number of the document. If a document is redacted, the text files shall not contain the redacted portions of the documents, but should contain the remaining

unredacted text.

d. **METADATA.** The following information shall be produced in the delimited data file accompanying hard copy documents: (a) BEGBATES, (b) ENDBATES, (c) CUSTODIAN, and (d) CONFIDENTIALITY.

e. **UNITIZING OF DOCUMENTS.** In scanning paper documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records (i.e., paper documents should be logically unitized). The parties will use reasonable efforts to unitize documents correctly to avoid producing large numbers of documents in single "clumps".

III. PRODUCTION OF ELECTRONICALLY STORED INFORMATION (ESI)

1. ESI production requests shall identify the custodian, search terms, and time frame relevant to the request.
2. ESI production requests shall only be propounded for specific issues, rather than general discovery of a product or business.
3. **TIMING.** The collection and production of ESI shall begin after the parties have exchanged initial disclosures and agreed to custodians, search terms, and relevant time periods.
4. **CUSTODIANS.** The parties shall meet and confer to reach agreement on a reasonable list of custodians and search terms for purposes of collection, review, and production of ESI. In connection with the meet and confer process, each party shall provide a proposed list of individual custodians who are knowledgeable about and were involved with the core issues or subjects in this case. The parties shall then meet and confer to reach agreement on the custodians to be collected from and relevant time periods for electronic searches of the files from those custodians.
5. **SEARCH TERMS.** Each producing party shall propose a list of search terms for

pending discovery requests. Search terms shall be narrowly tailored to particular issues. Indiscriminate terms, such as the producing company's name or its product name, are inappropriate unless combined with narrowing search criteria that sufficiently reduce the risk of overproduction. A conjunctive combination of multiple words or phrases (e.g., "computer" and "system") narrows the search and shall count as a single search term. A disjunctive combination of multiple words or phrases (e.g., "computer" or "system") broadens the search, and thus each word or phrase shall count as a separate search term unless they are variants of the same word. The parties shall then meet and confer to reach agreement on the search terms for electronic searches of the files from the previously agreed to custodians.

6. **CULLING\FILTERING.** Each party will use its best efforts to filter out common system files and application executable files by using a commercially reasonably hash identification process. Hash values that may be filtered out during this process are located in the National Software Reference Library ("NRSL") NIST hash set list. Additional culling of system file types based on file extension may include, but are not limited to: WINNT, LOGS, DRVS, MP3, C++ Program File (c) , C++ Builder 6 (cpp), Channel Definition Format (cdf), Creatures Object Sources (cos), Dictionary file (dic), Executable (exe), Hypertext Cascading Style Sheet (css), JavaScript Source Code (js), Label Pro Data File (IPD), Office Data File (NICK), Office Profile Settings (ops), Outlook Rules Wizard File (rwz), Scrap Object, System File (dll), Temporary File (tmp), Windows Error Dump (dmp), Windows Media Player Skin Package (wmz), Windows NT/2000 Event View Log file (evt), Python Script files (.py, .pyc, .pud, .pyw), and Program Installers.

7. **DEDUPLICATION.** Each producing party shall de-duplicate ESI on a global level (across all custodians) prior to production. The basis for such de-duplication shall be the MD5 or SHA1 Hash values, or some other later agreed to de-duplication method such as full text de-duplication. For generating either the MD5

or SHA1 hash values for email, the parties shall instruct their ESI processing vendors to take attachments into account for such hash value generation. The custodians of deduplicated copies of documents should be included in the database load file, either in the CUSTODIAN field or, alternatively, in a field for duplicative or other custodians (e.g. DUPE CUSTODIAN).

8. **STRUCTURED DATA.** The parties shall meet and confer with respect to structured data sources that contain relevant information to determine what information the reports should contain. As a general rule, data that is stored in a database, whether maintained internally by the party or through a third party provider, shall be produced as reports in Microsoft Excel, Microsoft Access or ASCII delimited text format.

9. **BACKUP DATA.** Absent a showing of good cause, no party need restore any form of media upon which backup data is maintained in a party's normal or allowed processes, including but not limited to backup tapes, disks, SAN, disaster recovery systems, and other forms of media, to comply with its discovery obligations in the present case.

10. **VOICEMAILS, INSTANT MESSAGES AND OTHER NON-EMAIL COMMUNICATION.** Absent a showing of good cause, voicemails, instant messages, communications via social media, PDAs, and mobile phones are deemed not reasonably accessible and need not be collected and preserved.

11. **PRODUCTION FORMAT FOR ESI.** The format of productions of ESI shall comply with the below listed requirements:

    a. **IMAGE FORMAT.** All documents covered by Sec. III of this stipulation shall be produced as single page black and white Group IV TIFFs, created with a resolution of at least 300 dots per inch (dpi), unless so excepted by Sec. III(11)(d). Color documents may be produced in .JPG format in lieu of TIFF images; where produced, color JPG files should also be provided

with a resolution of at least 300 dpi. Each TIFF or JPG image shall be branded with sequential production numbers and appropriate confidentiality designations. Each TIFF or JPG image filename shall correspond to the Bates number associated with that page. TIFF or jpg files shall show all text and images that would be visible to a user of the ESI documents.

i. **PRESENTATIONS.** The parties shall take reasonable efforts to process presentations (*e.g.*, PowerPoint) with hidden slides and speaker's notes unhidden, and to show both the slide and the speaker's notes on the TIFF of jpg image.

b. **DATABASE LOAD FILES/CROSS-REFERENCE FILES.** A production should be provided with (a) an ASCII delimited data file (.dat) using Concordance default delimiters, and (b) an Opticon (Concordance Image) image load file (.opt) that can be loaded into Concordance version 8 or above.

i. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the Image Load file(s) in the production.

ii. The Opticon file should provide the beginning and ending Bates number of each document and the number of pages it comprises. Each TIFF in a production must be referenced in the corresponding image load file.

iii. In addition to the metadata fields identified for production in Appendix 1 below, each .dat file shall include links to multi-page (document level) text files ("Text Path").

c. **TEXT FILES.** The multi-page text files described above in III(11)(b)(iii) shall include text extracted from ESI with extractable text. For electronic

files without extractable text (e.g. scanned paper documents, PDF files without text, etc.) or documents produced with redactions, the producing party shall use optical character recognition software (OCR) to generate text for the document. OCR generated text shall be provided for all documents without extractable text in the original native file unless the document is handwritten notes, drawings or is otherwise not easily convertible into a searchable format. The filename for the multi-page text file shall correspond to the beginning production number of the document.

d. **NATIVE FILES.** Any file produced in native format should be produced with a link in the NativeLink field, along with extracted full text and applicable metadata fields set forth in Appendix 1. Any file produced in native format should be named to match the beginning Bates number of their corresponding entries in the database load files. Additionally, every file produced natively should be accompanied by a Bates-stamped and confidentiality-stamped TIFF placeholder indicating the document was provided in native format. Only the files discussed below may be produced in native format unless both parties agree otherwise in writing.

i. **SPREADSHEETS.** Except for the placeholder referenced in III(11)(d) above, TIFF or JPG images of spreadsheets need not be produced unless redacted. Where produced in TIFF or JPG format, the parties will make reasonable efforts to ensure that any spreadsheets that are produced only as TIFF or JPG images are formatted so as to be readable.

ii. **VIDEO AND AUDIO FILES.** Audio and Video files will be produced in native format, with TIFF placeholders and available metadata provided in database load files.

iii. **EXCEPTIONS.** For any processing exception (i.e. a file that

cannot be processed by standard ESI processing tools) that is being produced due to document family relationships, the producing party shall provide a placeholder image that includes the file name of the document, a Bates number and a confidentiality designation, in addition to associated metadata.

iv. **REQUEST(S) FOR ADDITIONAL NATIVE FILES.** If good cause exists to request production of specified files, other than those specifically set forth above, in native format, the requesting party may request such production and provide an explanation of the need for native file review, which request shall not unreasonably be denied. Any native files that are produced should be produced with a link in the NativeLink field, along with all extracted text and applicable metadata fields, as well as a Bates-stamped and confidentiality-stamped TIFF placeholder. Any dispute regarding the production of documents in native format shall be resolved by the assigned magistrate judge, as set forth in the Standing Order for the Northern District of California, San Jose Division.

e. **METADATA FIELDS AND PROCESSING.** Each of the metadata and coding fields set forth in Appendix 1 that can be extracted shall be produced for each document. The parties are not obligated to populate manually any of the fields in Appendix 1 if such fields cannot be extracted from a document, with the exception of the following: (a) BEGBATES, (b) ENDBATES, (c) BEGATTACH, (d) ENDATTACH; (e) CUSTODIAN; and (f) CONFIDENTIALITY, which should be populated by the party or the party's vendor.

12. **FORMAT & FOLDER STRUCTURE.** The production data may be exchanged between counsel in encrypted form (*e.g.* TrueCrypt, password-protected Zip, or

RAR files). Productions of 10GB or less may be made via FTP or secure server; larger productions should be made on hard media (e.g., hard drives). Each production shall be provided in the following folder structure:

a. Top-level folder: This folder will indicate the production volume;

i. Sub-folders:

1. IMAGES: This folder will contain multiple sub-folders with ONLY TIFF (or .jpg) files in them. No other type of file should reside in the "IMAGES" folder. Sub-folders shall not contain more than 1000 images per folder.

2. TEXT: This folder will contain the full text files in UNICODE, UTF8 or ANSI format in a separate folder labeled TEXT. Sub-folders shall not contain more than 1000 text files per folder.

3. DATA: This folder will contain load files compatible with Concordance version 8 or above and Opticon.

4. NATIVES: This folder will contain native files that the parties agree to produce during the course of this litigation. Sub-folders shall not contain more than 1000 native files per folder.

IV. DISCLOSURE AND REVIEW OF SOURCE CODE

1. Source code means human-readable programming language text that defines software, firmware, or electronic hardware descriptions as well as any and all programmer notes, annotations, and other comments of any type related thereto and accompanying the code.

2. Any source code that a producing party produces shall be made available to persons authorized to have access to source code pursuant to Section IV of this agreement, unless otherwise mutually agreed to by the parties.

3. Source code must be produced in its native format pursuant to the following provisions:

a. Source code, to the extent any producing party produces such information, shall ONLY be made available for inspection in electronic native format at the offices of the producing party's primary outside counsel of record in this action, or at a location mutually agreed upon by the receiving and producing parties.

b. Source code will be loaded on two (2) non-networked computers (equipped with a separate monitor) that are password protected and maintained in a secure, locked area. Source code may be loaded onto more than two non-networked computers upon agreement by the producing party or upon application of the receiving party after showing good cause.

c. Use or possession of any input/output device (e.g., USB memory stick, cameras or any camera-enabled device, CDs, floppy disk, portable hard drive, laptop, etc.) is prohibited while accessing the computer containing the source code.

d. The computers containing source code will be available for inspection during regular business hours, upon reasonable notice to the producing party, which shall not be less than three (3) business days in advance of the requested inspection.

e. Should the producing party transfer source code to the source code computers on more than one occasion, each set of source code files shall be located within a separate folder, which is titled with at least the date the source code was transferred to the source code computer, such that the receiving party is able to identify the files produced on a particular occasion based on their location within the date-titled folder(s).

f. The producing party shall identify the programming language(s) and operating system(s) used to develop or edit any files installed on the source code computers (which shall be appropriate to the file types and

technologies of the files produced) at the time the producing party indicates the source code is available for inspection.

g. The producing party shall install any tools for viewing, searching, and analyzing the source code produced on the platform produced, if such tools exist and are presently used in the ordinary course of the producing party's business and are reasonably necessary for the receiving party's outside counsel and/or experts to review the relevant source code. The receiving party's outside counsel and/or experts may request that additional commercially available licensed software tools for view, searching, and analysis of source code be installed on the secured computer, and must provide the producing party with the CD or DVD containing such software tool(s) at least four business days in advance of the inspection.

h. The receiving party's outside counsel and/or expert shall be entitled to take notes relating to the source code but may not copy any portion of the source code into the notes. The receiving party's outside counsel and/or experts are permitted to (i) make and/or maintain electronic copies of their notes outside of the source code review room; and (ii) take such notes on the source code computer itself provided that such notes are not transmitted outside the source code review room and are deleted upon conclusion of the review. Any such notes shall be treated as though designated as source code under the protective order, and shall be afforded the same protections contained therein. No copies of all or any portion of the source code may leave the room in which the source code is inspected except as otherwise provided herein. Further, no other written or electronic record of the source code is permitted except as otherwise provided herein.

i. No person shall copy, e-mail, transmit, upload, download, print, photograph or otherwise duplicate any portion of the designated source

code without the agreement of the producing party or further order of the Court.

j. A list of names, relationship to the case, and qualifications of persons who will view the source code will be provided to the producing party in conjunction with any written (including email) notice requesting inspection. The producing party shall maintain a daily log of the names of persons who enter the locked room to view the source code and when they enter and depart. The producing party may visually monitor the activities of the receiving party's representatives during any source code review, but only to ensure that there is no unauthorized recording, copying, or transmission of the source code.

k. Unless otherwise agreed in advance by the parties in writing, following each inspection, the receiving party's outside counsel and/or experts shall remove all notes, documents, and all other materials from the room that may contain work product and/or attorney-client privileged information. The producing party shall not be responsible for any items left in the room following each inspection session.

l. The receiving party will not copy, remove, or otherwise transfer any portion of the source code from the source code computer including, without limitation, copying, removing, or transferring any portion of the source code onto any other computers or peripheral equipment. The receiving party will not transmit any portion of the source code in any way from the location of the source code inspection.

m. No person shall copy, e-mail, transmit, upload, download, print, photograph or otherwise duplicate any portion of the designated source code, except that the receiving party may request a reasonable number of pages of source code to be printed by the producing party, but only if and

to the extent necessary for use in this action in a court filing, pleading, expert report, or other paper, or for deposition or trial. The printed pages shall constitute part of the source code produced by the producing party in this action. In no event may the receiving party print more than 35 consecutive pages, or an aggregate total of more than 500 pages, of source code during the duration of the case without prior written approval by the producing party or the Court's approval. Within 3 business days, or such additional time as necessary due to volume requested, the producing party will provide two copies of the requested source code on watermarked or colored paper bearing bates numbers and the appropriate confidentiality branding under the protective order. Contested source code printed pages need not be produced to the receiving party until the matter is resolved by the Court.

n. Any printed pages of source code, and any other documents or things reflecting source code that have been designated by the producing party as source code pursuant to the protective order may not be copied, digitally imaged or otherwise duplicated, except in limited excerpts necessary to attach as exhibits to depositions, expert reports, or court filings as discussed above.

o. The parties shall not provide the court reporter with copies of source code that are marked as deposition exhibits and such exhibits shall not be attached to deposition transcripts; rather, the deposition record will identify the exhibit by its production numbers.

p. Except as provided in this paragraph, the receiving party may not create electronic images, or any other images, of the source code for use on a computer (e.g., may not scan the source code to a PDF, or photograph the code). A receiving party may include excerpts of source code in a

pleading, exhibit, expert report, discovery document, deposition transcript, other Court document, or any drafts of these documents (hereinafter a "source code document"). The receiving party shall only include such excerpts as are reasonably necessary for the purposes for which such part of the source code is used. The receiving party may create an electronic image of a selected portion of the source code only when the electronic file containing such image has been encrypted using commercially reasonable encryption software including password protection. The communication and/or disclosure of electronic files containing any portion of source code shall at all times be limited to individuals who are authorized to see source code under the provisions of the protective order.

q. To the extent portions of source code are quoted or otherwise disclosed in a source code document, either (1) the entire document will be stamped with the appropriate source code designation as defined in the protective order or (2) those pages containing quoted source code will be separately bound, and stamped with the appropriate source code designation as defined in the protective order. All source code documents shall be filed under seal, according to the provisions of the protective order, such that source code is redacted in any publicly available document or filing. A receiving party shall make a good faith effort to quote the minimum amount of source code necessary in any such document.

4. Miscellaneous

a. The producing party may not configure its source code in a manner that unreasonably impedes or slows the receiving party's ability to inspect the source code or allows the producing party to monitor the receiving party's inspection (e.g., key logging, video capture, etc.).

b. Images or copies of source code shall not be included in correspondence

between the parties (references to production numbers shall be used instead), and shall be omitted from pleadings and other papers whenever possible.

c. All cumulative paper or electronic copies of source code shall be securely destroyed in a timely manner if they are no longer in use (e.g., at the conclusion of a deposition).

d. Access to and review of source code shall be strictly for the purpose of investigating the claims and defenses at issue in this case. No person shall review or analyze any source code for purposes unrelated to this case, nor may any person use any specific knowledge gained as a result of reviewing source code in this case in any other pending or future dispute, proceeding, patent prosecution, or litigation.

e. The receiving party shall comply with any applicable export controls under the laws of the United States and agrees not to knowingly export, re-export, or transfer source code of the producing party without first obtaining all required United States or any other applicable authorizations or licenses.

V. PRIVILEGE LOGS

1. For all documents withheld on the basis of privilege, the parties agree to furnish logs which comply with the legal requirements under federal law, but at a minimum will include the following information:

a. A unique number for each entry on the log.

b. The date of document. For emails this should be the sent date of the document and for loose ESI this should be the last-modified or create date of the document.

c. The Author of the document. For emails this should be populated with the metadata extracted from the "Email From" field associated with the file. For loose ESI, this should be populated with the metadata extracted from the "Author" field; if such field contains generic information such as the company name, a party may substitute the

information contained in the "Custodian" metadata field.

d. Recipient(s) of the document where reasonably ascertainable. For emails this should be populated with the metadata extracted from the "Email To" field associated with the file. Separate columns should be included for the metadata extracted from the "Email CC" and "Email BCC" fields, where populated.

e. A description of why privilege is being asserted over the document. This description should include information sufficient to identify if the document contained attachments over which privilege is also being asserted.

f. The type of privilege being asserted: (a) AC for Attorney/Client, (b) WP for Attorney Work Product, (c) CI for Common Interest.

2. The parties shall identify on their logs where counsel is present in conversation, specifically for columns 1(c) and (d) noted above. Where counsel creating the privilege is not readily ascertainable from columns 1(c) and (d) above, the parties shall include a reference to counsel in the privilege description field described in 1(e) above.

3. Privilege logs may be produced on a rolling basis or after all productions are complete, but prior to the close of discovery. If the log(s) are produced after all productions are complete, the receiving party shall have thirty (30) days from the date of receipt to review and register complaints about said log(s), regardless of the date of the close of fact discovery.

VI. REDACTION LOGS

1. For each document that is redacted, in addition to providing the redacted version of the document, the parties agree to furnish logs which comply with the legal requirements under Federal Law, but at a minimum will include the following information:

a. The Begin Production ID of the document.

b. The End Production ID of the document.

c. A description of why privilege is being asserted over the document, or some other explanation as to why the document was redacted, such as "Not Responsive to RFPs".

d. If the document was redacted for privilege concerns, the type of privilege being

asserted: (a) AC for Attorney/Client, (b) WP for Attorney Work Product, (c) CI for Common Interest.

2. Redaction logs may be produced on a rolling basis or after all productions are complete, but prior to the close of discovery. If the log(s) are produced after all productions are complete, the receiving party shall have thirty (30) days from the date of receipt to review and register complaints about said log(s), regardless of the date of the close of fact discovery.

VII. EXCEPTION TO LOGGING - POST FILING DATE PRIVILEGE DOCS

Communications involving inside or outside counsel for the parties related to this case or any of the other Related Cases described in the Joint Case Management Statement, and materials withheld from discovery on grounds of privilege, work product or similar doctrines, that were created on or after December 5, 2014, need not be included in the parties privilege log(s) as a matter of course. These exceptions are made without prejudice to any party's ability and right to assert that such materials are discoverable and not privileged or protected. These exceptions also do not apply to the redacted documents and their respective redaction log(s).

VIII. INADVERTENT PRODUCTION OF PRIVILEGED INFORMATION.

Pursuant to Federal Rule of Evidence 502(d), the inadvertent production of privileged or work product protected data is not a waiver in the pending case or in any other federal or state proceeding. The receiving party shall not use produced data that the producing party asserts is attorney-client privileged or work product protected to challenge the privilege or protection. The mere production of privileged information in a litigation as part of a mass production shall not itself constitute a waiver for any purpose.

In addition, the inadvertent production of any privileged document, information or thing shall not be deemed a waiver of such privilege or otherwise affect the producing party's right to seek return of the inadvertently produced document, information, or thing. The party receiving the document(s) that appears to be privileged shall promptly notify the producing party upon becoming aware that the document(s) may have been inadvertently produced and in any event, before making use of said document.

In the event that documents which are claimed to be privileged or subject to the work-product doctrine are inadvertently produced, such documents shall be returned by the receiving party within two (2) calendar days of any written request therefore. The receiving party shall return all copies of the inadvertently produced document(s) and not retain any copies, notes, or summaries of said documents. If the receiving party seeks to challenge the privileged nature of the document(s), the receiving party must still return the document(s) to the producing party but may then seek re-production of the document(s).

It is the desire, intention and mutual understanding of the parties that all inadvertently or unintentionally disclosed or produced privileged information shall be treated as confidential and may not be disclosed by the receiving party to persons or entities other than the producing party without the written consent of the producing party.

If a party who received documents or information over which a privilege is asserted has disclosed such documents or information to any person or in any circumstance, the party must immediately: (a) notify, in writing, the producing party of the disclosure; (b) use best efforts to retrieve all copies of the documents or information over which the privilege is asserted; and (c) notify, in writing, the producing party regarding whether all copies have been retrieved.

The parties further agree that no motion to compel or other argument for waive of privilege will be raised based upon the inadvertent or unintentional production or disclosure of privileged information.

Nothing herein shall prevent the receiving party from challenging the propriety of the claim of attorney client privilege, work product protections or other applicable privilege or immunity designation by submitting a written challenge to the court.

IX. COMMUNICATIONS WITH EXPERTS

Drafts of reports, declarations, or affidavits prepared by an expert who may give testimony in this case or one of the Related Cases discussed in Section 10 below ("Testifying Expert"), or his or her assistants, as part of the Testifying Expert's investigation and/or in developing the Testifying Expert's opinions and reports shall not be subject to discovery. This limitation applies

regardless of whether such draft reports have been disclosed, or otherwise transmitted to, or contain any notes, writing, or markings created by in-house counsel or outside counsel, or employees of or consultants for the party or parties who engaged such Testifying Expert.

Notes and other documents prepared by a Testifying Expert, or his or her assistants, as part of the investigation and/or in preparing an expert report shall not be subject to discovery.

Discovery of materials provided to Testifying Experts is limited to those materials, facts, consulting expert opinions, and other matters actually relied upon by the Testifying Expert in formulating his/her final report(s), trial or deposition testimony or any opinion in the above-captioned Investigations.

No discovery may be taken from any consulting expert that will not provide testimony and/or an expert opinion in this case or the Related Cases discussed in Section 10 below ("Consulting Expert"), including with respect to drafts of reports, if any, prepared by an expert except to the extent that the Consulting Expert has provided information, opinions, or other materials that a Testifying Expert relied on in formulating his/her final report(s), trial or deposition testimony, or any opinion in the above-captioned Investigations. Where a Consulting Expert has provided materials or information that a Testifying Expert has relied on in formulating his/her final report(s), trial or deposition testimony, or any opinion, discovery (other than depositions) may be taken of the Consulting Expert regarding those specific materials and information. The limitations herein do not preclude a party from discovery of prior opinions or testimony of an expert in matters other than the above-captioned Investigations, to the extent the prior opinions or testimony are related to and/or may be inconsistent with the opinions given in the above-captioned Investigations.

Written or oral communications between any Testifying Expert or Consulting Expert, his or her assistants, and/or in-house counsel or outside counsel, or employees of or consultants for the party or parties who engaged such Testifying Expert or Consulting Expert, are not subject to discovery unless the conversations or communications are relied upon by a Testifying Expert in

formulating his/her final report(s), trial or deposition testimony, or any opinion in the above-captioned Investigations.

Notwithstanding the foregoing, experts reports must disclose all documents and things considered or relied upon by the expert with reference to this case, including definitions and possible prior art, and including any documents or things provided by counsel or by the expert's staff, although communications forwarding or otherwise concerning such source documents or things are not discoverable.

X. MISCELLANEOUS

This Stipulation is entered into without prejudice to the right of any party to apply to the Court at any time for modification of this Stipulation. Furthermore, without application to this Court, the parties may agree in a signed writing to modify the terms of this Stipulation.

DATED: May 21, 2015

Respectfully submitted,

/s/ Sean S. Pak

Kathleen Sullivan (SBN 242261)
kathleensullivan@quinnemanuel.com
QUINN EMANUEL URQUHART & SULLIVAN LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Sean S. Pak (SBN 219032)
seanpak@quinnemanuel.com
John M. Neukom (SBN 275887)
johnneukom@quinnemanuel.com.
Matthew D. Cannon (SBN 252666)
matthewcannon@quinnemanuel.com
QUINN EMANUEL URQUHART & SULLIVAN LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Mark Tung (SBN 245782)
marktung@quinnemanuel.com
QUINN EMANUEL URQUHART &

SULLIVAN LLP
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Steven Cherny *(admission pro hac vice pending)*
steven.cherny@kirkland.com
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Adam R. Alper (SBN 196834)
adam.alper@kirkland.com
KIRKLAND & ELLIS LLP
555 California Street
San Francisco, California 94104
Telephone: (415) 439-1400
Facsimile: (415) 439-1500

Michael W. De Vries (SBN 211001)
michael.devries@kirkland.com
KIRKLAND & ELLIS LLP
333 South Hope Street
Los Angeles, California 90071
Telephone: (213) 680-8400
Facsimile: (213) 680-8500

Attorneys for Plaintiff Cisco Systems, Inc.

DATED: May 21, 2015

Respectfully submitted,

/s/ Robert A. Van Nest

KEKER & VAN NEST LLP
ROBERT A. VAN NEST - # 84065
rvannest@kvn.com
BRIAN L. FERRALL - # 160847
bferrall@kvn.com
DAVID J. SILBERT - # 173128
dsilbert@kvn.com
MICHAEL S. KWUN - # 198945
mkwun@kvn.com
633 Battery Street
San Francisco, CA 94111-1809
Telephone:415 391 5400
Facsimile: 415 397 7188
Attorneys for Defendant Arista Networks, Inc.

ATTORNEY ATTESTATION

I hereby attest, pursuant to Local Rule 5-1(i)(3), that the concurrence in the filing of this document has been obtained from the signatory indicated by the "conformed" signature (/s/) of Robert A. Van Nest within this e-filed document.

/s/ *Sean S. Pak*

Appendix 1: ESI Metadata and Coding Fields

A. **Imagebase Load File (.opt) shall be in Concordance Image/Opticon (.opt) format and include a record for each page with the following fields:** ALIAS, VOLUME, PATH, DOC_BREAK, FOLDER_BREAK, BOX_BREAK, PAGES

B. **Metadata Load File (.dat)** shall include a record for each document and use Concordance default delimiters, as follow:

Field Delimiter = (ASCII 020)
Text Delimiter = þ (ASCII 254)
Line Delimiter = ® (ASCII 174)

C. The following fields will appear in the metadata load file in the order displayed below:

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family
CUSTODIAN	Individual from whom the documents originated
SUBJECT	Subject line of email
DATESENT	Date email was sent (format: MM/DD/YYYY)
TIMESENT	Time email was sent
DATERCVD	Date on which email message was received (MM/DD/YYYY)
TIMERCVD	Time at which email message was received
FROM	The name and email address of the sender of the email
TO	All recipients that were included on the "To" line of the email
CC	All recipients that were included on the "CC" line of the email
BCC	All recipients that were included on the "BCC" line of the email
CONVERSATIONINDEX	The conversation index extracted from the produced email message where available
AUTHOR	Any value populated in the Author field of the document properties
LASTAUTHOR (Edoc only)	Last author or editor of document, from document properties

Field Name	Field Description
FILENAME(Edoc only)	Filename of an electronic document
FILEEXT	File extension
FILEPATH	Path to file or message
FILESIZE	The original file size of the produced document
DATELASTMOD (Edoc only)	Date an electronic document was last modified (format: MM/DD/YYYY)
TIMELASTMOD	Time at which document was last modified
DATECREATED (Edoc only)	Date the document was created (format: MM/DD/YYYY)
TIMECREATED	Time at which document was created
TITLE	Title of document, from document properties
CONFIDENTIALITY	All Confidentiality designations
PAGE COUNT	The number of pages of the produced document
MD5HASH	A calculated value unique to each identical file. The producing party may substitute the SHA1 Hash value, but will name the field accordingly to indicate such substitution
TEXTLINK	Path to the associated multi-page/document level text file for each produced document
NATIVELINK	Path to the associated native file where applicable
PRODVOLUME	The production volume associated with the produced file